

What is claimed is:

1. A method of managing a network session comprising:
  - delivering policies from a server to a remote system that has predetermined configuration information;
  - establishing a secure connection between the server and the system; and
  - regulating activities in the system based on at least one of the set of policies and the predetermined configuration information.
2. The method of claim 1 wherein regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria.
3. The method of claim 2 wherein the rejection criteria include the predetermined static configuration information.
4. The method of claim 2 wherein the rejection criteria include the set of policies.
5. The method of claim 1 wherein regulating the activities comprises providing a session layer adapted to reject unauthorized data packets based on context such as user and application information.
6. The method of claim 1 wherein regulating the activities comprises:
  - providing a session layer adapted to reject unauthorized data packets based on context information; and
  - providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

1 7. The method of claim 1 further comprising updating the set  
2 of policies.

1 8. The method of claim 1 further comprising:  
2 detecting data packets from the regulated activities; and  
3 rejecting the data packets from the regulated activities.

1 9. An article comprising a computer-readable medium which  
2 stores computer-executable instructions for managing a network  
3 session, the instructions causing a computer to:

4 receive a set of policies from a server in a remote  
5 system having predetermined configuration information;

6 establish a secure connection between the server and the  
7 system; and

8 manage activities in the system based on at least one of  
9 the set of policies and the predetermined configuration  
10 information.

11 10. The article of claim 9, further comprising updating the  
12 set of policies.

13 11. The article of claim 9 wherein the instructions to reject  
14 the intervening processes comprises instructions to provide  
15 filters that are adapted to reject data packets based on  
16 rejection criteria.

17 12. The article of claim 11 wherein the rejection criteria  
18 includes predetermined static configuration information.

19 13. The article of claim 11 wherein the rejection criteria  
20 includes the set of policies.

21 14. The article of claim 9 wherein the instructions to reject  
22 the unauthorized activities comprises instructions to provide  
23 a session layer adapted to reject unauthorized data packets  
24 based on context user and application information.

1 15. The article of claim 9 wherein the instructions to reject  
2 the unauthorized activities comprises instructions to:

3 provide a session layer adapted to reject unauthorized  
4 data packets based on context information; and

5 provide filters adapted to reject unauthorized data  
6 packets based on rejection criteria from at least one of the  
7 context information and the policies.

1 16. The article of claim 9, further comprising instructions  
2 to:

3 detect unauthorized data packets from the unauthorized  
4 activities; and

5 reject the unauthorized data packets from the  
6 unauthorized activities.

17. A network system, comprising:

first and second devices, wherein the first device is  
adapted to:

deliver a set of policies to the second device;

and the second device is adapted to:

detect data packets from unauthorized activities;

and

reject the data packets from the unauthorized  
activities.

1 18. The system of claim 17 further comprising a network  
2 stack.

1 19. The system of claim 18, wherein the network stack  
2 comprises:

3 a policy engine connected to the first device;

a policy store connected to the policy engine;  
a socket interceptor connected to the policy engine; and  
a packet guard connected to the policy engine.

20. The system of claim 17, the first device further comprising instructions to monitor the system for the intervening processes.

21. A network stack, comprising:

a policy engine;  
a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;  
a socket interceptor coupled to the policy engine;  
a packet guard coupled to the policy engine.

22. The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard.

23. The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server.

24. The network stack of claim 23 further comprising a configurable management process adapted to reconfigure the network stack and having instructions to:

receive policies in the policy engine from the policy server;

use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications;

10 use the packet guard to filter unauthorized activities  
11 received from the network interface;

12 use the packet guard to filter the data packets from  
13 unauthorized users and applications based on the context  
14 information received by the socket interceptor; and

15 use the packet guard to filter data packets based on the  
16 policies.

00T EEO\* 8266E560